(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 March 2002 (07.03.2002)

PCT

(10) International Publication Number
WO 02/19593 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/SE01/01814

(22) International Filing Date: 24 August 2001 (24.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/651,364 30 August 2000 (30.08.2000) US

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: **MARIZ-RIOS, Jose-Luis**; Bronce 37, 4-19, E-28045 Madrid (ES). **RUIZ-SANCHEZ, Jose-Luis**; Rosas de Aravaca 82F-2D, E-28032 Madrid (ES). **SCHUBERTH, Ulf**; Alstömergatan 31, 5tr, S-112 47 Stockholm (SE). **KNORR, Jürgen**; C/Violeta Parra 6 Portal 3 6b, E-28903 Getafe (Madrid) (ES).

(74) Agent: **MAGNUSSON, Monica**; Ericsson Radio Systems AB, Patent Unit Radio Access, S-164 80 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/19593 A2

(54) Title: SERVICE PROVIDER-INDEPENDENT SAT-BASED END-USER AUTHENTICATION

(57) Abstract: A system and method for verifying the identity of an end-user. The end-user requests to access an external application. The external application sends an authentication request to an authentication server, which generates a random token. The generated token is transmitted to the end-user. The end-user enters the generated token and a personal identification number into a cellular terminal connected to a GSM network. At least the token is encrypted using a secret key stored within the cellular terminal and transmitted through the GSM network to an authentication gateway. The token is decrypted by the authentication gateway using either the same secret key or a key matched to the secret key. The token is then transmitted to the authentication server where the received key is compared to the generated key. The results of the comparison are transmitted to the external application.

SERVICE PROVIDER-INDEPENDENT SAT-BASED END-USER AUTHENTICATION

BACKGROUND

The present invention relates generally to methods and apparatus for providing end-user authentication services for network access providers and more particularly methods and apparatus that apply network security procedures to authenticate users who are requesting access to network applications.

The number of users who access data networks from remote locations increases each day. In many cases, a data network provider may wish to restrict network access to a group of users (such as customers, employees, etc.) and thereby create a private network. A private network is typically a network in which access to host sites of the private network is limited to authorized users. When a private network is connected to a public network, security procedures, including authentication procedures, should be carried out to ensure that only authorized users from authorized hosts can gain access to the private network. For example, when a user requests access to a host site of the private network from a remote location, the user must be authenticated before the user is granted access to the host site.

Some conventional authentication procedures use passwords. A password is a string of characters that may be recognized by automatic means to permit a user to access protected files or other system resource. Most sophisticated systems use authentication schemes based on passwords.

A password may be generated at a remote site that is requesting access to a host site of the private network. Some systems utilize either symmetric or asymmetric cryptographic techniques to create and authenticate the password.

The continuous development of data networks has generated a wide range of computer services. In some cases, the services are restricted to a number of users providing service on a first-come, first-served basis. In other cases, the services are accessed on a commercial basis, i.e., the users pay to utilize the services. In the latter case, users must authenticate themselves using a service provision system of a service provider before they can gain access to the desired services. Typically, this requires the user to provide a unique username and password. The service provider verifies the username and password entered by the user against a database maintained by the service provider and grants access if the entered

information matches the information in the database. In this manner, the service provider ensures that only users entitled to access the services can do so.

Cellular communication systems control resources of a network in a similar fashion. For example, in a Global System for Mobile Communication ("GSM") network, the mobile station (e.g., GSM phone) includes a Subscriber Identity Module ("SIM"). The SIM contains subscriber information, including data that permits the mobile station to gain access to the GSM network and utilize subscriber-based function of the network (e.g., calling party identification, voice mail, etc.).

Remote access to public or private data networks is growing tremendously, especially through dial-up connections such as public switched telephone networks ("PSTN") or the higher speed integrated services digital networks ("ISDN"). However, these dial-up connections are inherently insecure because they transmit data over open communication lines. Additionally, software for breaching security is quite advanced and more widely used than it was in the past. For example, software is available for guessing the passwords of authorized users of the network. Network diagnostic equipment can also be used to capture the user names and passwords of authorized users. Once user names and passwords become known, unauthorized users can pose as authorized users and gain access to the network. This problem can be overcome by using known authentication techniques.

Weak authentication, also known as single-factor authentication, uses a single method to authenticate a user. Weak authentication encompasses static passwords and one-time passwords. Static passwords can be broken by software programs, including keyboard strike monitoring programs, cracking programs for guessing passwords, and network sniffing programs. Static passwords can be protected from such software programs by generating a one-time password (one per session) that can not be calculated from previous passwords, e.g., by using a pseudo-random sequence as a calculation factor. The one-time password is generated from a "real" password that would never be transmitted over the network, and such a "real" password thus constitutes secret data that is shared by the user and the network.

Strong authentication, also known as two-factor authentication, is safer than weak authentication because it authenticates the user by two methods, typically a token and a password. Systems that generate one time passcodes from a token and a password are already available in the market, such as Security Dynamic's Secure ID, Safeword's Safeword DES Gold Card, and Digital Pathway's Defender. For example, the token may be a hardware

device and the password may be a Personal Identification Number ("PIN") code needed to access the hardware device. The token typically contains some unique identification code. A passcode is generated by encrypting the user's PIN and the token's identification code. The network would then use the passcode to verify the user's identity.

Strong authentication can be made still safer, for example, by introducing explicit authentication, in which the network generates a random factor as input to the user's password generation operation. This is known as a "challenge-response" procedure, in which the network challenges the user to give a correct response. Second, the life of the passcode can be short, e.g., one minute, and the authentication process can be repeated periodically during the session. Third, more sophisticated keys and algorithms, based either in symmetric or asymmetric cryptography, can be used. Nevertheless, increased sophistication usually requires additional time and processing power to perform the authentication task.

Both weak and strong authentication techniques have limitations. For example, static login/password methods provide weak security, and strong authentication methods require a user to hold additional devices, i.e., token devices. Some strong authentication mechanisms require specific hardware, e.g., smart card readers. Furthermore, some strong authentication methods require specific hardware and software configurations that create administrative burdens.

Some of these limitations and burdens can be overcome, or at least made more acceptable to the user, by combining different forms of authentication. For example, the token can be embedded in the hardware needed to access the network, like embedding a SIM card in a GSM phone.

Reliable authentication can also be achieved by using two different communication channels. One communication channel can be used to access a private service network and the other communication channel can be used to authenticate the user requesting access. In this case, one of the communication channels can be an unsecured channel connected to a data network over an access network and the other communication channel can be a secured channel that would exchange security information between a mobile station and the data network over a Public Land Mobile Network ("PLMN"). Under these circumstances, the authentication would take place over the secure channel, making it more difficult to steal authentication information. Once the authentication is completed, the secure channel would be released and could be used by others.

Such an authentication scheme could be implemented using a GSM network as the secured communication path. This is discussed in commonly assigned, co-pending U.S. Patent Application No. 09/386,253, which was filed on August 31, 1999, by José Luis Mariz Rios and José Luis Ruiz Sánchez, entitled "GSM Security for Packet Data Networks", and which is incorporated in its entirety here by reference.

In GSM, the provider of cellular communication services ("GSM Service Provider") identifies the end-user by a SIM in the end-user's cellular terminal. The SIM, based on smart-card technology, is personalized and distributed to the end-user by the GSM Service Provider.

The GSM-based identification of end-users can be re-used for applications that reside outside of the cellular system ("External Applications"). A typical implementation is shown in Figure 1. The end-user 100 uses a remote access device, such as a computer 102, to send an access request 104 to an External Application 106 through an Access Network 108, such as the Internet. The access request 104 is forwarded to an Authentication Server 110 that identifies the end-user 100 through his/her Cellular Terminal 112 via communication over the GSM network 114. Typical examples of External Applications 106 that can utilize GSM-based authentication schemes include Internet services that require safe identification of the end-user, such as Internet banking and remote access to corporate local area networks ("LANs").

A simple authentication scheme is based on the generation of a Token 116 in the Authentication Server 110. The Token 116, typically a number or alphanumeric string that is preferably randomly generated, is sent in plain text over the GSM network 114 to the cellular terminal 112 of the end-user 100. The end-user 100 returns this Token 116 to the External Application 106 using the computer 102 connected to the External Application 106 through the access network 108. If the generated and returned Token is the same, the result of the authentication is positive. The advantage with such simple authentication schemes is that they are straightforward to implement and can be operated and controlled by the provider of the External Application, with minimal involvement of the GSM Service Provider.

More advanced authentication solutions can be implemented using SIM Application Toolkit ("SAT") technology. With SAT, the GSM Service Provider can store tailor-made software on the SIM card ("SAT Application"). The Authentication Server communicates with the SAT application over the GSM network, and identifies the end-user via an interaction on the cellular terminal. The result of the authentication procedure is

communicated to the External Application.

An issue associated with SAT-based authentication mechanisms is that the GSM Service Provider and the provider of the External Application may be separate entities. This creates concerns regarding the division of liabilities between the entities, and a question of "who should control what" in the security chain.

The GSM Service Provider issues the SIM card, and, for security purposes, may desire to retain the control of this component. Hence, the GSM Service Provider is the only entity that will have access to the SIM card to insert SAT applications. A SAT-based authentication mechanism requires a back-end Authentication Server, and from the perspective of the GSM Service Provider, the Authentication Server should remain under the control of the GSM Service Provider. For example, in a symmetric authentication solution, the Authentication Server will contain the same secret key of the end-user as the one stored on the SIM card, and can therefore not be under the control of an external party.

The provider of the External Application, on the other hand, requires (in the majority of cases) to be in control of the authentication procedure for the External Application, and the associated end-user data base. From this perspective, it is the provider of the External Application that should control the Authentication Server.

These and other drawbacks of previous systems and methods are alleviated by Applicants' invention that provides service provider-independent SAT-based authentication.

SUMMARY

In accordance with one aspect of the present invention, there is provided a system to authenticate an end-user. The system comprises an external application in communication with a first communication device through a first communication network. An authentication server is also in communication with the external application. The authentication server is adapted to receive an authentication request from the external application in response to an access attempt by the first communication device. The authentication server generates a token in response to the authentication request and sends the token through the external application to the first communication device. An authentication gateway is in communication with a second communication device through a second communication network. The authentication gateway is adapted to receive a token from the second communication device and transmit the token to the authentication server. When the token is

received from the authentication gateway, the received token is compared to the token generated by the authentication server.

In accordance with another aspect of the present invention, the token is generated and verified by the authentication server, the authentication server and external application being controlled by a first common entity. The token may be encrypted throughout all communication paths, and the authentication server can simultaneously support encrypted and unencrypted tokens. A secret key may be stored in an authentication gateway, and the secret key may be used to decrypt the token transmitted from the first communication device to the authentication gateway, the authentication gateway and the first communication network being controlled by a second common entity.

In accordance with other aspects of the present invention, the first common entity may be distinct from the second common entity, and advertisements related to the external application can be presented to the end-user via the first communication device.

In accordance with yet another aspect of the present invention, a method for authenticating an end-user comprises the steps of requesting access to an External Application; sending an authentication request from the External Application to the Authentication Server; generating a random Generated Token in the Authentication Server; presenting the Generated Token to the end-user via the External Application; and entering the end-user's PIN and the Generated Token. The method further includes calculating a cryptographic response based on the PIN, Generated Token, and Secret Key, and the calculation uses a cryptographic algorithm and the Secret Key resides within the SAT application; transmitting the response to an Authentication Gateway and an Authentication Server. The method still further includes decrypting the response with the Secret Key in the Authentication Gateway and decrypting the response with the PIN in the Authentication Server, with the decrypted response resulting in a Returned Token. In addition, the Returned Token is compared with the Generated Token, and access to the External Application may be granted if the Returned Token and the Generated Token are the same and if the Returned Token is received within a pre-defined time.

In accordance with another aspect of the present invention, there is a network architecture for authenticating an end-user. The network comprises at least one gateway connected to at least one communication network, wherein the at least one gateway provides authentication services to the at least one communication network. In addition, there is at

least one server connected to at least one external application, wherein the at least one server provides authentication services to the at least one external application. At least one switch connects the at least one gateway to the at least one server, wherein any of the at least one gateways is accessible, through the at least one switch, by the at least one server.

In accordance with another aspect of the present invention, there is a system for authenticating an end-user. The system comprises an external application in communication with a first communication device through a first communication network. An authentication server is in communication with the external application. The authentication server receives an authentication request from the external application in response to an access attempt by the first communication device. The authentication server generates a token in response to the authentication request and sends the token through the external application to the first communication device. An authentication gateway is in communication with a second communication device through a second communication network. The authentication gateway receives a first message from the second communication device and transmits a second message to the authentication server. The first message is based on the token and an end-user's PIN code, and the second message is compared to a result of a computation based on the token generated by the authentication server and a PIN code stored in the authentication server and associated with the end-user.

BRIEF DESCRIPTION OF THE DRAWINGS

The features, objects, and advantages of the present invention will become apparent by reading this description in conjunction with the accompanying drawings, in which:

Figure 1 is a block diagram that illustrates a method of authenticating a user known to the art;

Figure 2 is a block diagram that illustrates a method of authenticating a user according to an exemplary embodiment of the present invention;

Figure 3 is a block diagram that illustrates a method of implementing a service to provide user authentication to a plurality of External Applications through a plurality of GSM networks; and

Figure 4 is a flow diagram of the method for authenticating an end-user.

DETAILED DESCRIPTION

In the following description, the invention is described in terms of a GSM communication system, but it will be understood that Applicants' invention is not so limited. The invention can be embodied in other types of communication systems that have appropriate features.

In accordance with one aspect of the present invention, there is provided a SAT-based authentication method, whereby end-user authentication is based on three components: a secret PIN, a Secret Key, and a random number (Token). Control of these components is divided between two nodes: an Authentication Gateway (under the control of the GSM Service Provider), and an Authentication Server (under the control of the provider of the External Application). Preferably, communication between the Authentication Gateway and Authentication Server is encrypted. An exemplary architecture is depicted in Figure 2.

The PIN includes a secret string of keystrokes (e.g., an alphanumeric string) that is known by the end-user. The PIN can be stored and/or checked in the Authentication Gateway, in the Authentication Server, or locally on the SIM card. The Secret Key is stored on the SIM-card in connection with the SAT application and, in the case of symmetric keys, in the Authentication Gateway. The Token (e.g., a random numeric or alphanumeric string) is generated and checked in the Authentication Server.

As can be appreciated, there are two possible authentication scenarios: Mobile Initiated and Network Initiated.

In the Mobile Initiated scenario, an end-user 200 requests access (via an access request 202) to the External Application 204 and identifies himself/herself, e.g., by his/her Mobile Subscriber ISDN number ("MSISDN ") or other suitably unique user name. Typically, an access device 208 transmits an access request 202 to an External Application 204 through an access network 206. As will be appreciated, the access network 206 can be a GSM network, a PSTN, or other communication network, including a LAN. Access device 208 can be any suitable network terminating device, including, for example, telephones, computers, and personal digital assistants ("PDA").

The External Application 204 sends an authentication request 210 to the Authentication Server 212. The Authentication Server 212 generates a random Token 214 and presents the Token to the end-user 200 via the External Application 204. The end-user 200 reads the Token 214 from the External Application 204 and may select an "Authentication-option" from a menu on the authenticating device 216 (this option can be

presented on the menu with the SAT application). The SAT application advantageously prompts the end-user 200 for a PIN and then for a Token. After the end-user 200 has entered the PIN and Token, the SAT application generates a response based on the PIN, Token, and Secret Key, using a predetermined cryptographic algorithm (e.g., Triple DES). If the PIN is stored/checked locally on the SIM, the response may be based only on the Token and Secret Key. The authenticating device 216 sends the response 218 back to the Authentication Gateway 222 via the GSM network 220. The response 218 is decrypted with the Secret Key (and the PIN, if available) in the Authentication Gateway 222, which forwards the decrypted response, now a Returned Token, to the Authentication Server 212. (If the PIN is stored in the Authentication Server 212, then the response forwarded from the Authentication Gateway 222 to the Authentication Server 212 is decrypted by the Authentication Server 212 to produce the Returned Token.) The Authentication Server 212 compares the Returned Token with the Generated Token. If the correct Token is returned within a pre-defined period of time (e.g., one minute), the result of the authentication request is positive and is communicated to the External Application 204 in the form of an authentication result 224.

As can be appreciated, the Returned Token can be generated using non-reversible cryptographic algorithms. For example, a common cryptographic transformation, such as a hash function, that uses the Generated Token and/or PIN as input can be used to calculate the Returned Token. The Authentication Server 212 may also use the same hash function to calculate the expected response, again based on the Generated Token and/or PIN. The expected response would then be compared to the Returned Token.

The Network Initiated scenario differs from the Mobile Initiated case in the way the SAT dialogue on the authenticating device 216 is activated. In the Mobile Initiated scenario (described above), the SAT dialogue is initiated by the end-user, e.g., by selecting an "Authentication-option" from a menu displayed on the cellular terminal. In the Network Initiated scenario, the dialogue is initiated from the Authentication Server 212, via the Authentication Gateway 222, and further to the SIM card/cellular terminal via a message sent from the Authentication Gateway 222 over the GSM Network.

Figure 4 is a flowchart of the steps of a method of authenticating an end-user that is in accordance with Applicants' invention. First, in step 401, an External Application receives an access request. Typically, this access request will be the result of an end-user's actively accessing the External Application, such as an internet banking website. In response to the

access request, the External Application sends an authentication request to an Authentication Server in step 402. As can be appreciated, the Authentication Server and the External Application may both be software tasks running on the same computer, or they may be on separate computers connected by a network. The network may be a LAN or a telecommunication network.

In step 403, the Authentication Server generates a Token that preferably token is a pseudo-random sequence, e.g., of numbers and letters. The Token, in step 404, is transmitted to the accessing device. Typically, the end-user reads the Token from the accessing device and enters it into the authenticating device. The end-user may also need to enter a PIN into the authentication device to verify his identity, but the Token could also be transmitted without user intervention by cable, infra-red, or radio-frequency methods known to the art.

Once the Token is entered into the authenticating device, the authenticating device generates a cryptographic response based on the Token, a Secret Key resident in the authenticating device, and possibly the PIN (step 405). The Secret Key is preferably embedded within the authentication device, but may also be encoded in a smart card or other access card that is held by the end-user and read by the authentication device.

In step 406, the response is sent to an Authentication Gateway and the Authentication Server. In step 407, the Authentication Gateway decrypts the response based on the Secret Key. The Authentication Server decrypts the Token based on the PIN or, if the PIN is not used in generating the response, the Authentication Server receives the Token from the Authentication Gateway. As previously noted, one-way algorithms, such as hash functions, can also be used in place of reversible cryptographic algorithms. If the received Token matches the generated Token, access to the External Application is granted. The Authentication Server may also require that the response be received in a pre-determined period of time. If this is required and the response is received late, access to the external application may be denied.

As can be appreciated, the Token should be long enough so that it cannot be guessed by an intruder within the time allowed for response. In addition, the length of the Token is related to the cryptographic function used to combine it with the PIN and the encryption algorithm in the SIM-Authentication Gateway communication. On the other hand, the Token should also be short enough so that the end-user can successfully enter it into the authenticating device within the allowed response time.

As can be appreciated, Applicants' invention has significant benefits over the prior art. For example, the provider of the External Application is in control of the Authentication Server and the associated end-user database (MSISDNs, and optionally, the associated user names and/or PINs). In addition, the provider of the External Application has the final control of the authentication procedure (comparing the Generated and Returned Token in the Authentication Server). This ensures that the provider of the External Application has full control over access to its content.

While the provider of the External Application retains control of the application, the Service Provider remains in control of the SIM card, SAT application, and the associated Secret Key. Via the Authentication Gateway, the GSM Service Provider gains access to a prime advertising channel. Advertisements related to accessed External Applications can be presented to the end-user via a SAT interaction on the Cellular Terminal.

The Token is transported in encrypted form throughout the transmission path SIM - GSM Network - Authentication Gateway - Authentication Server. In addition, every authentication request results in strong two-factor authentication of the end-user: it is verified that the end-user knows the PIN, and holds the SIM card. In case the PIN is stored and checked locally on the SIM card or in the Authentication Gateway, the end-user will only need to remember one password (PIN) for all External Applications that utilize the authentication method. Also, in case the MSISDN is used as user name, there will not be any need to remember application-specific user-names.

The Authentication Server in the proposed SAT-based scheme performs the same Token-based authentication check as in simple solutions, where the Token is sent in clear text over the GSM network. This makes it possible to support both solutions in the same Authentication Server. It also enables smooth migration from the simple solution to the more advanced SAT-solution, as more and more end-users acquire SAT-enabled SIMs (and Cellular Terminals).

A method of service-provider independent authentication is complicated by the fact that there are currently more than 350 GSM networks in operation, a number that is constantly increasing. For a provider of an External Application, whose end-users can have subscriptions with any GSM network, relations must be maintained with a large number of GSM networks. This is needed both for simple authentication schemes (based on sending random Tokens in clear text over GSM), as well as for the more advanced SAT-based

mechanism just described. The solution is to launch an operator-independent Authentication Service.

Figure 3 is an exemplary network architecture that could be used to provide an Authentication Service. The provider of the Authentication Service supplies Authentication Servers 310a, 310b, 310c, 310d, 310e, 310f to providers of External Applications 320a, 320b, 320c, 320d, 320e, 320f, such as Internet banks, enterprises offering remote intranet/extranet access, providers of high-valued Internet content, etc. These Authentication Servers 310a-310f can preferably support both the simple, clear-text Token-based authentication mechanism, as well as the more advanced SAT mechanism. In addition, each Authentication Server 310a-310f can concurrently service more than one External Application 320a-320f. Preferably, it is the responsibility of the provider of the External Application 320a-320f to register end-users in a database, indicate which GSM Service Provider 330a, 330b, 330c, 330d each subscribes to, and which authentication mechanism each uses.

The Authentication Service also supplies Authentication Gateways 340a, 340b, 340c, 340d, 340e to GSM Service Providers 330a-330d to handle the SAT-based authentication mechanism. As can be appreciated, Authentication Gateways 340a-340e can also be made available for a network-based authentication mechanism for networks other than GSM.

In addition, the Authentication Service operates one or more central switches 350 to provide simplified connectivity between providers of External Applications 320a-320f and GSM Service Providers 330a-330d. While the system shown in Figure 3 employs only one switch, the system could be duplicated to accommodate multiple switches with appropriate inter-switch connectivity. A variety of inter-switch connection schemes are known to the art. The Authentication Service is also responsible for monitoring the overall quality and security of the service, including the connections between the Authentication Servers 310a-310f and Authentication Gateways 340a-340e.

Various embodiments of the invention have been described, and those skilled in the art will likely make additional embodiments of this invention. For example, the first and second access device and network can be the same, thereby allowing an External Application to be accessed by a mobile phone. In addition, the invention can be embodied in other network technologies. For example, mobile networks that use a subscriber module, analogous to a SIM, to identify an end-user can use Applicants' invention. In addition, additional services, such as advertising, can be provided to the GSM device during the

authentication process. These and other alternate embodiments are intended to fall within the scope of the claims which follow.

WE CLAIM:

1. A system for authenticating an end-user, comprising:

an external application in communication with a first communication device through a first communication network;

an authentication server in communication with the external application, the authentication server being adapted to receive an authentication request from the external application in response to an access attempt by the first communication device, and the authentication server generating a token in response to the authentication request and sending the token through the external application to the first communication device; and

an authentication gateway in communication with a second communication device through a second communication network, the authentication gateway being adapted to receive a token from the second communication device and to transmit the token to the authentication server, wherein the token received from the authentication gateway is compared to the token generated by the authentication server.

2. The system of claim 1, wherein the authentication server and external application are controlled by a first common entity.

3. The system of claim 1, wherein the authentication server and the external application are controlled by different entities.

4. The system of claim 1, wherein the token is encrypted throughout all communication paths.

5. The system of claim 4, wherein the authentication server can simultaneously support encrypted and unencrypted tokens.

6. The system of claim 5, wherein a secret key is stored in an authentication gateway, the secret key is used to decrypt the token transmitted from the first communication device to the authentication gateway, and the authentication gateway and the first communication network are controlled by a second common entity.

7. The system of claim 6, wherein the first common entity is distinct from the second common entity.

8. The system of claim 7, wherein advertisements related to the external application are presentable to the end-user via the second communication device.

9. The system of claim 7, wherein the second communication network is a GSM network.

10. A method for authenticating an end-user, comprising the steps of:

sending an authentication request from an external application to an authentication server;

generating a token in the authentication server;

presenting the generated token to a first communication device via the external application;

generating a cryptographic response based on at least the generated token and a secret key residing within a second communication device;

transmitting the cryptographic response from the second communication device to an authentication gateway and the authentication server;

decrypting the cryptographic response in the authentication gateway and the authentication server to provide a returned token;

comparing the returned token with the generated token; and

granting access to the external application if the returned token corresponds to the generated token.

11. The method of claim 10, wherein the returned token must be received by the authentication server within a pre-determined time period.

12. A network architecture for authenticating an end-user, comprising:

at least one gateway connected to at least one communication network, wherein the at least one gateway provides authentication services to the at least one communication network;

at least one server connected to at least one external application, wherein the at least one server provides authentication services to the at least one external application; and

at least one switch connecting the at least one gateway to the at least one server, wherein any of the at least one gateways is accessible, through the at least one switch, by the at least one server.

13. The network architecture of claim 12, wherein each of the at least one gateways is controlled by a unique entity.

14. A system for authenticating an end-user, comprising:

an external application in communication with a first communication device through a first communication network;

an authentication server in communication with the external application, the

authentication server receiving an authentication request from the external application in response to an access attempt by the first communication device, and the authentication server generating a token in response to the authentication request and sending the token through the external application to the first communication device; and

an authentication gateway in communication with a second communication device through a second communication network, the authentication gateway receiving a first message from the second communication device and transmitting a second message to the authentication server;

wherein the first message is based on the token and an end-user's PIN code, and the second message is compared to a result of a computation based on the token generated by the authentication server and a PIN code stored in the authentication server and associated with the end-user.

15. The system of claim 14, wherein the first message is based on the token, the end-user's PIN code, and a secret key.

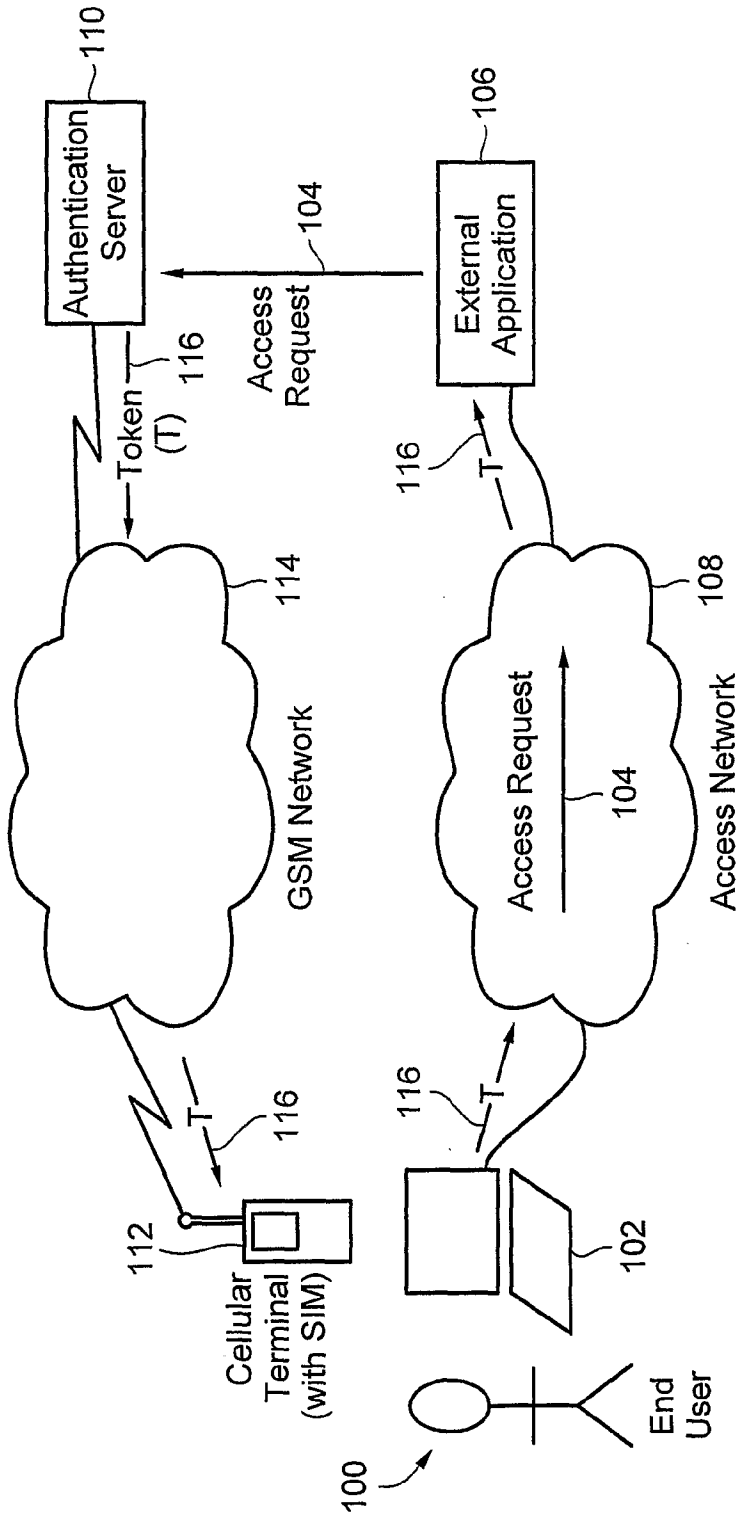


FIG. 1
PRIOR ART

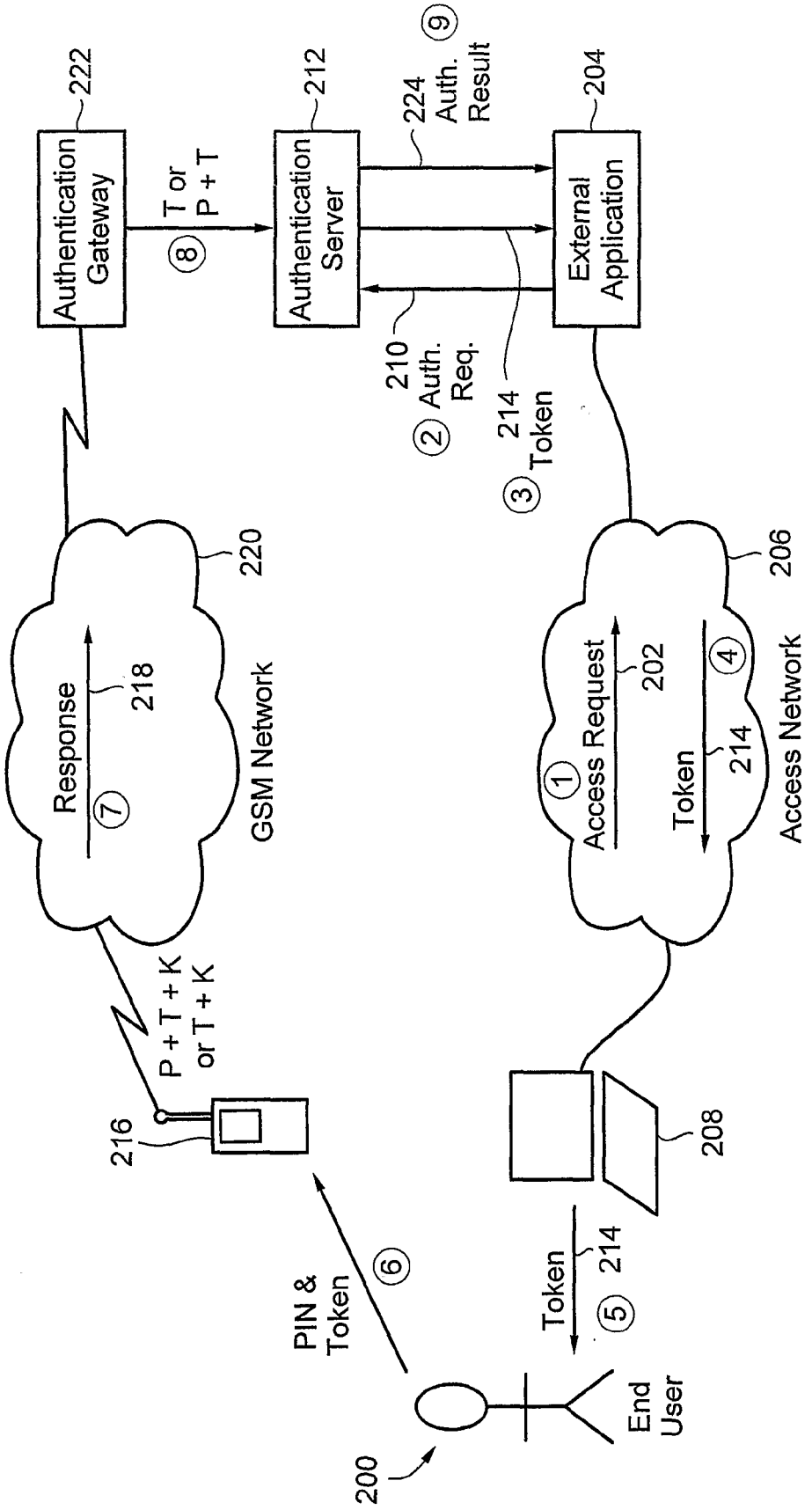

Authentication Gateway
222
T or P + T
8
Authentication Server
212
224 Auth. Result
9
External Application
204
210 Auth. Req.
2
214 Token
3
Response
7
218
GSM Network
220
Access Request
1
202
Token
214
4
Access Network
206
P + T + K or T + K
216
208
PIN & Token
6
Token
214
5
End User
200

FIG. 2

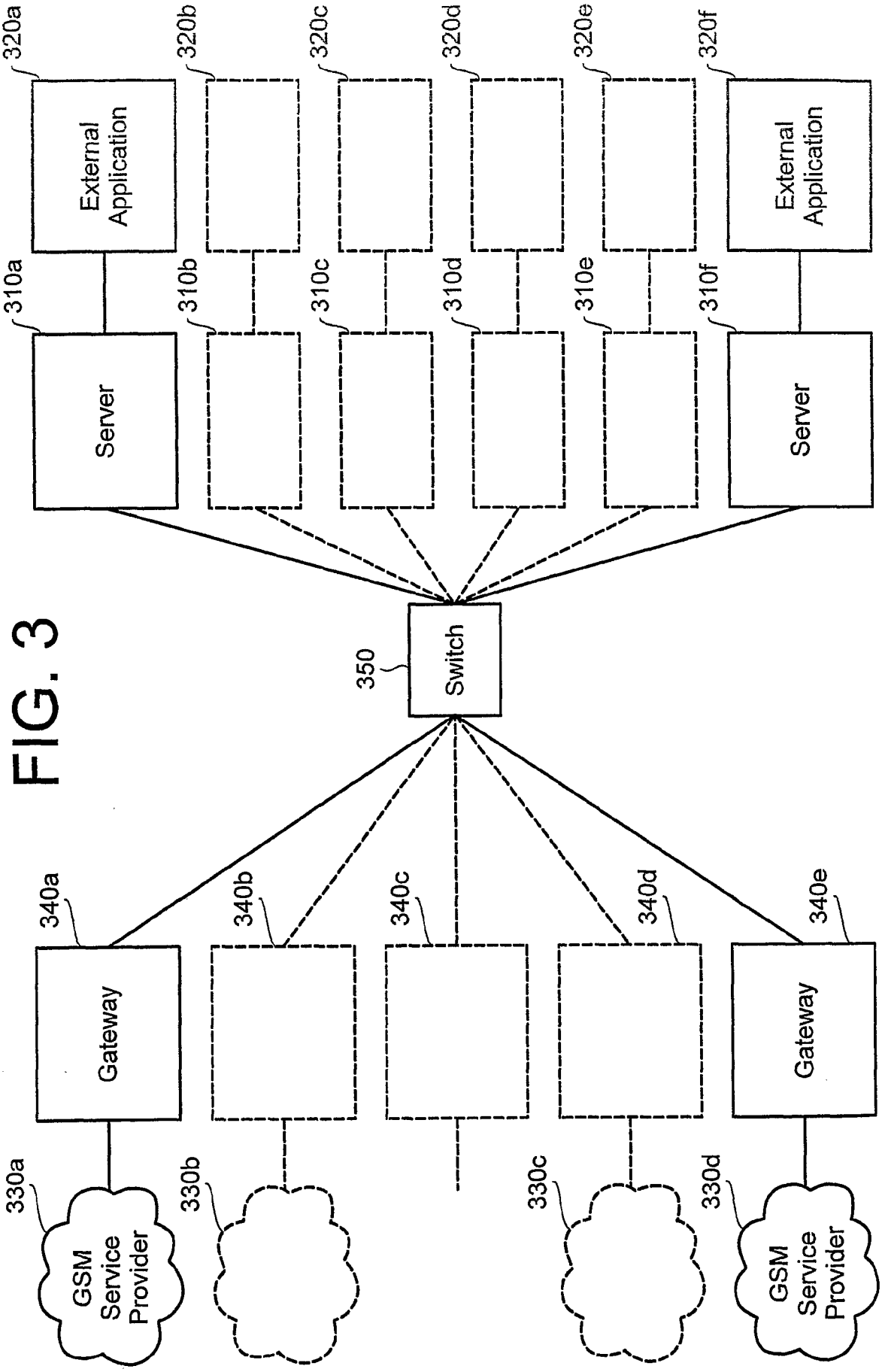

320a
External Application
320b
320c
320d
320e
320f
External Application
310a
Server
310b
310c
310d
310e
310f
Server
350
Switch
340a
Gateway
340b
340c
340d
340e
Gateway
330a
GSM Service Provider
330b
330c
330d
GSM Service Provider

FIG. 3

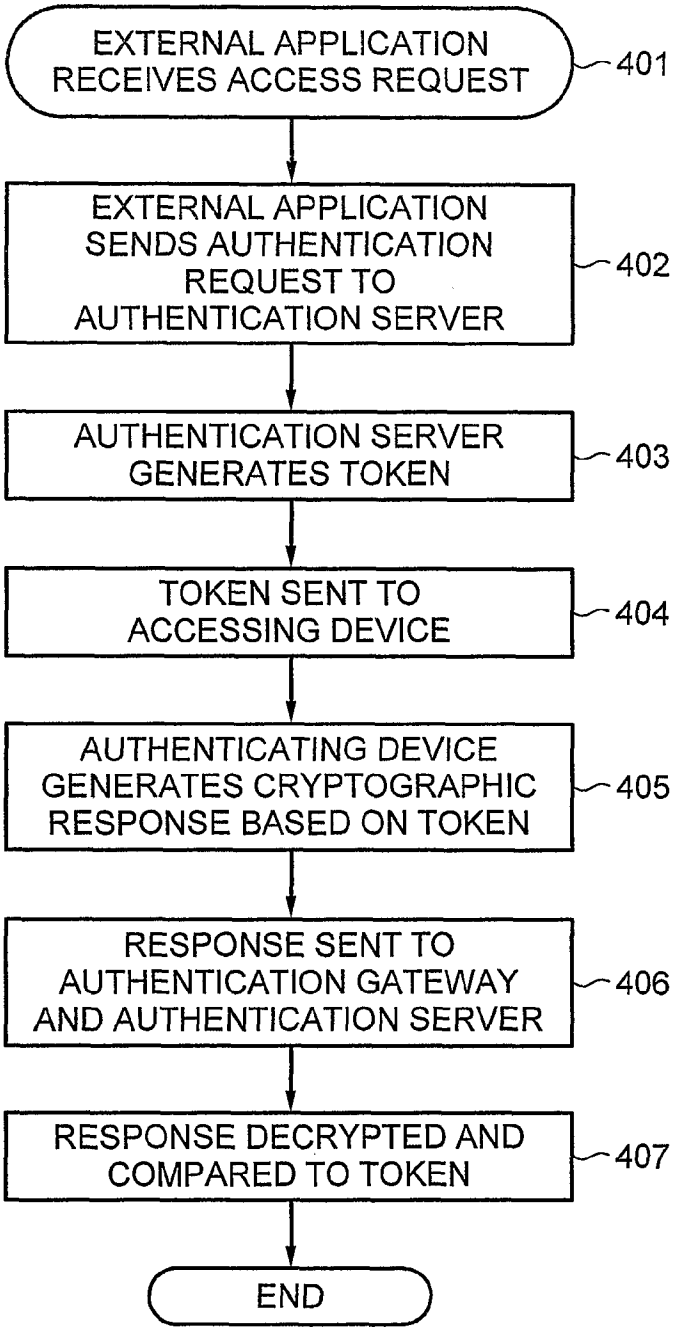

EXTERNAL APPLICATION RECEIVES ACCESS REQUEST
401
EXTERNAL APPLICATION SENDS AUTHENTICATION REQUEST TO AUTHENTICATION SERVER
402
AUTHENTICATION SERVER GENERATES TOKEN
403
TOKEN SENT TO ACCESSING DEVICE
404
AUTHENTICATING DEVICE GENERATES CRYPTOGRAPHIC RESPONSE BASED ON TOKEN
405
RESPONSE SENT TO AUTHENTICATION GATEWAY AND AUTHENTICATION SERVER
406
RESPONSE DECRYPTED AND COMPARED TO TOKEN
407
END

FIG. 4

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 March 2002 (07.03.2002)

PCT

(10) International Publication Number
WO 02/019593 A3

(51) International Patent Classification[7]: H04L 9/32, H04Q 7/24, H04L 29/06

(74) Agent: MAGNUSSON, Monica; Ericsson AB, Patent Unit Radio Access, S-164 80 Stockholm (SE).

(21) International Application Number: PCT/SE01/01814

(22) International Filing Date: 24 August 2001 (24.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/651,364 30 August 2000 (30.08.2000) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: MARIZ-RIOS, Jose-Luis; Bronce 37, 4-19, E-28045 Madrid (ES). RUIZ-SANCHEZ, Jose-Luis; Rosas de Aravaca 82F-2D, E-28032 Madrid (ES). SCHUBERTH, Ulf; Alstömergatan 31, 5tr, S-112 47 Stockholm (SE). KNORR, Jürgen; C/Violeta Parra 6 Portal 3 6b, E-28903 Getafe (Madrid) (ES).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

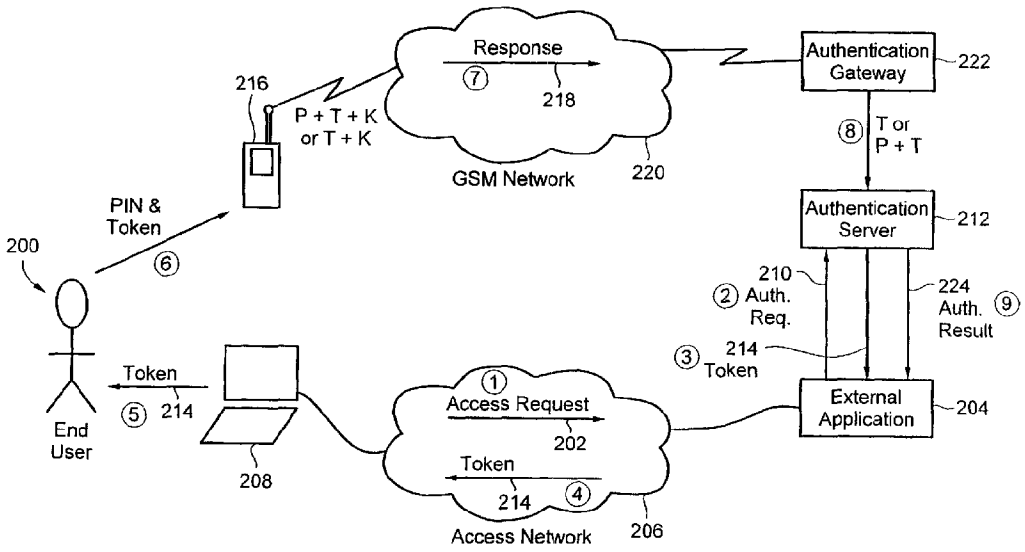
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
6 September 2002

[Continued on next page]

(54) Title: END-USER AUTHENTICATION INDEPENDENT OF NETWORK SERVICE PROVIDER



(57) Abstract: A system and method for verifying the identity of an end-user. The end-user requests to access an external application. The external application sends an authentication request to an authentication server, which generates a random token. The generated token is transmitted to the end-user. The end-user enters the generated token and a personal identification number into a cellular terminal connected to a GSM network. At least the token is encrypted using a secret key stored within the cellular terminal and transmitted through the GSM network to an authentication gateway. The token is decrypted by the authentication gateway using either the same secret key or a key matched to the secret key. The token is then transmitted to the authentication server where the received key is compared to the generated key. The results of the comparison are transmitted to the external application.

WO 02/019593 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Inter ıal Application No
PCT/SE 01/01814

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04Q7/24 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 668 876 A (FALK JOHAN PER ET AL) 16 September 1997 (1997-09-16) abstract column 3, line 1 - line 50 column 4, paragraph 3 column 5, line 23 - line 55	1-5,10, 14,15
A	column 8, line 41 - line 64; figure 1A ---	6-9,11
E	WO 02 01516 A (AUCSHITH DAVID ;INTEL CORP (US); SULLIVAN ROBERT JR (US)) 3 January 2002 (2002-01-03) abstract page 8, paragraph 4 -page 10, paragraph 1 --- -/--	1-3

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 May 2002	28/05/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Blanco Cardona, P

INTERNATIONAL SEARCH REPORT

Inter ıal Application No
PC1/3E 01/01814

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 44114 A (ERICSSON TELEFON AB L M) 2 September 1999 (1999-09-02) abstract page 9, paragraph 3 page 13, paragraph 3 page 15, paragraph 3 -page 16, paragraph 2 page 19, paragraph 3 -page 21, paragraph 1 page 23, paragraph 4 -page 24, paragraph 1	1-15
A	US 6 078 908 A (SCHMITZ KIM) 20 June 2000 (2000-06-20) abstract column 2, line 57 -column 3, line 55	4,5
A	WO 00 44130 A (BERGGREN ULF ;NETCOM AB (SE)) 27 July 2000 (2000-07-27) abstract page 5, line 26 -page 6, line 6 claims 1,16	1-15
A	US 6 061 650 A (KOSSACK NANCY ET AL) 9 May 2000 (2000-05-09) abstract column 2, line 26 -column 4, line 49 column 5, line 35 - line 39; figure 1	12,13

INTERNATIONAL SEARCH REPORT

rmation on patent family members

Inter ıal Application No
PC /SE 01/01814

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5668876 A	16-09-1997	AU 692881 B2	18-06-1998
		AU 2688795 A	19-01-1996
		CA 2193819 A1	04-01-1996
		EP 0766902 A2	09-04-1997
		FI 965161 A	13-02-1997
		JP 10502195 T	24-02-1998
		WO 9600485 A2	04-01-1996
WO 0201516 A	03-01-2002	WO 0201516 A2	03-01-2002
WO 9944114 A	02-09-1999	FI 980427 A	26-08-1999
		AU 2831699 A	15-09-1999
		BR 9908246 A	31-10-2000
		CN 1292108 T	18-04-2001
		EE 200000491 A	15-02-2002
		WO 9944114 A1	02-09-1999
		EP 1058872 A1	13-12-2000
		JP 2002505458 T	19-02-2002
US 6078908 A	20-06-2000	DE 19718103 A1	04-06-1998
		AU 6354598 A	05-11-1998
		BR 9801177 A	20-03-2001
		CN 1207533 A	10-02-1999
		EP 0875871 A2	04-11-1998
		JP 10341224 A	22-12-1998
		TW 425804 B	11-03-2001
WO 0044130 A	27-07-2000	SE 516066 C2	12-11-2001
		AU 2335900 A	07-08-2000
		WO 0044130 A1	27-07-2000
US 6061650 A	09-05-2000	NONE	